Rewriting Homework
A rendre au plus tard le 8 janvier 2016

In what follows \( \mathcal{R} \) is a finite term rewriting system on the function symbols \( \mathcal{F} \). \( \mathcal{F} \) is assumed to contain infinitely many constant symbols \( \{ a_i \mid i \in \mathbb{N} \} \), which we do not recall in the examples.¹ We use the symbol \( \top \) for an empty set of equations, or the identity substitution.

We recall that an idempotent substitution \( \phi \) is a mapping from a finite set of variables \( \text{Dom}(\phi) \) (called its domain) to \( T(\mathcal{F}, X \setminus \text{Dom}(\phi)) \). A solution (in the free algebra) of a set of equations either has no solution or has an idempotent mgu (most general unifier) \( \mu \) such that \( \mu \) is a solution and all other solutions \( \sigma \) can be written \( \sigma = \mu \theta \). Deciding whether there is a solution or not, and, in case there is one, computing an idempotent mgu, can be completed in linear time.

An mgu \( \{ x_1 \mapsto u_1; \ldots; x_k \mapsto u_k \} \) is identified with a solved system \( x_1 =_0 u_1 \land \ldots \land x_k =_0 u_k \).

The goal here is to extend unification procedures to solve equations in quotients \( T(\mathcal{F})/ \xrightarrow{\mathcal{R}} \) where \( \mathcal{R} \) is a confluent term rewriting system.

An equation system \( S \) is a formula
\[
\exists x_1, \ldots, x_m. \ u_1 =_{\mathcal{R}} v_1 \land \ldots \land u_n =_{\mathcal{R}} v_n \quad \parallel \quad \phi
\]
where \( u_1, \ldots, u_n, v_1, \ldots, v_n \in T(\mathcal{F}, X) \), and \( \phi \) is an idempotent substitution (the solved part of the system), whose domain is disjoint from \( \{ x_1, \ldots, x_n \} \).

All equations are assumed to be symmetric: we make no distinction between \( u =_{\mathcal{R}} v \) and \( v =_{\mathcal{R}} u \) (resp. \( u =_0 v \) and \( v =_0 u \)).

A solution of an equation system \( \exists x_1, \ldots, x_m. \ u_1 =_{\mathcal{R}} v_1 \land \ldots \land u_n =_{\mathcal{R}} v_n \quad \parallel \quad \phi \) is a substitution \( \sigma \) from \( \text{Dom}(\sigma) \subseteq \text{Var}(u_1, v_1, \ldots, u_n, v_n, \phi) \setminus \{ x_1, \ldots, x_m \} \) to \( T(\mathcal{F}) \) such that there is a substitution \( \theta \), from \( x_1, \ldots, x_m \) to \( T(\mathcal{F}) \), such that

1. for every \( i = 1, \ldots, n \),
\[
\frac{u_\sigma \theta}{\mathcal{R}} v_\sigma \theta
\]

2. there is a substitution \( \theta' \) such that, \( \sigma \theta = \phi \theta' \)

An equation system is in solved form if it is of the form \( \exists \overline{x}. \ T \quad \parallel \quad \phi \).

Consider the following transformation rules, in which the variables of the rules in \( \mathcal{R} \) are renamed each time it is necessary.

**(Block)\)** \( \exists \overline{x}. \ u =_{\mathcal{R}} v \land S \quad \parallel \quad \phi \rightsquigarrow \exists \overline{x}. \ S \sigma \quad \parallel \quad \sigma \)

If \( \sigma \) is a m.g.u. of \( u =_0 v \land \phi \)

**(Narrow)\)** \( \exists \overline{x}. \ u =_{\mathcal{R}} v \land S \quad \parallel \quad \phi \rightsquigarrow \exists \overline{x}, \overline{y}. \ u[p]_\sigma =_{\mathcal{R}} v \sigma \land S \sigma \quad \parallel \quad \sigma \)

if \( \overline{y} = \text{Var}(l \mapsto r), \ l \mapsto r \in \mathcal{R}, \)
\( p \) is a non-variable position of \( u, \)
\( \sigma \) is a m.g.u. of \( l =_0 u[p] \land \phi, \)
\( \overline{y} \cap \text{Var}(u, v, S) = \emptyset \)

¹Adding such constant symbols, standing for the variables in \( T(\mathcal{F}, X) \) prevents from confusing the syntax of the problems and their interpretation. It is not a restriction on the problems that are considered.
A derivation is a sequence of equation systems $E_i$ such that $E_0 \rightsquigarrow \cdots \rightsquigarrow E_i \rightsquigarrow \cdots$ and each derivation step relies on one of the two above rules. The solved forms of an equation system $S$ are all systems $S'$ in solved form that can be obtained by a derivation starting with $S$.

We will show below that this yields a procedure for solving equation systems for an arbitrary convergent $\mathcal{R}$.

**Question 1**
Consider the following (ground) rewrite system on $\mathcal{F} = \{f(1), g(1), a(0), b(0)\}$

$$\mathcal{R}_0 = \begin{cases} f(g(a)) \rightarrow f(b) \\ g(f(b)) \rightarrow g(a) \end{cases}$$

and the equation system $E_0 = f(g(x)) \equal{R} f(y) \parallel \top$.

Give all possible derivations starting from $E_0$ and yielding a solved form.

**Question 2**
Consider the following rewrite system on $\mathcal{F} = \{\text{enc}(2), \text{dec}(2), \pi_1(1), \pi_2(2), \langle \_ \_ \rangle (2)\}$:

$$\mathcal{R}_1 = \begin{cases} \text{dec}(\text{enc}(x, y), y) \rightarrow x \\ \pi_1(\langle x, y \rangle) \rightarrow x \\ \pi_2(\langle x, y \rangle) \rightarrow y \end{cases}$$

Give all possible derivations starting from $\pi_1(\text{dec}(x, y)) \equal{R} y \parallel \top$. (2 possible derivations).

**Question 3**
Show that, if $S \rightsquigarrow S'$, then the solutions of $S'$ are contained in the solutions of $S$.

**Question 4**
1. Assume that $\mathcal{R}$ is terminating and confluent. A substitution $\sigma$ is then normalized if, for every variable $x$, $x\sigma$ is irreducible.

Show that, if $\sigma$ is a normalized solution of $E = \exists x. S \parallel \phi$, $S\phi = S$ and $S \neq \top$, then there is a $E'$ such that $E \rightsquigarrow E'$ and $\sigma$ is a solution of $E'$.

2. Show that any normalized solution of an equation system $S \parallel \top$ is a solution of one of its solved forms.

Deduce a procedure for solving equations in the quotient $T(\mathcal{F})/\xrightarrow{\mathcal{R}}$ for convergent rewrite systems $\mathcal{R}$.

3. Give an example showing that this result is incorrect when $\mathcal{R}$ is terminating but not confluent.

4. Give an example of a confluent $\mathcal{R}$, an equation system $E = u \equal{R} v \parallel \top$ and a solution $\sigma$ such that for every $E'$ such that $E \rightsquigarrow E'$ and for every $\sigma'$ such that, for every variable $x$, $x\sigma' \not\equal{R} x\sigma$, $\sigma'$ is not a solution of $E'$. (Hence termination is necessary)
Question 5

Consider the rewrite system

\[ \mathcal{R}_2 = \left\{ \begin{array}{l} 0 + x \rightarrow x \\ s(x) + y \rightarrow s(x + y) \end{array} \right. \]

1. Explain why \( \mathcal{R}_2 \) is confluent

2. Using the automatic procedure of the previous question, give the solved forms of the equation systems

(a) \( x + y \overset{?}{=} s(s(0)) \).

(b) \( x + 0 \overset{?}{=} s \)

Question 6

We replace here the Narrow rule with

\[ \text{(Narrow)} \quad \exists \bar{x} \quad u \overset{?}{=} v \wedge S \quad || \quad \phi \quad \leadsto \exists \bar{x}, \bar{y} \quad u[r] \overset{?}{=} v \wedge S \quad || \quad \sigma \]

if \( \bar{y} = \text{Var}(l \rightarrow r) \), \( l \rightarrow r \in \mathcal{R} \)

\( p \) is a non-variable position of \( u \),

\( \sigma \) is a mg.u. of \( l \overset{?}{=} v \mid \phi \),

\( \bar{y} \cap \text{Var}(u, v, S) = \emptyset \)

In other words, the unifier \( \sigma \) is not applied to the unsolved part of the equations. (This is known as the basic strategy).

1. Show that this restriction is harmless: in case \( \mathcal{R} \) is convergent, the results of the questions 3 and 4 still hold true with this strategy.

2. How does it help for the examples of question 5?

Question 7

Show that, if \( \mathcal{R} \) is confluent and if every right hand side of a rule is a subterm of the corresponding left-hand side, then the procedure derived from question 6 is terminating.

Would it be also the case with the procedure derived from question 4?